Exhibit M: P&N Information Security

Information Security Processes and Qualifications

As an accounting and business advisory firm, confidentiality is a hallmark of our profession and it is of the utmost importance to our client relationships. At P&N, we are committed to keeping client data secure which is why we have designed engagement tools and policies to help ensure information security and privacy.

P&N employs professionals that maintain numerous information technology and data security certifications as well as a Service Organization Control (SOC) services team that has substantial experience in performing SOC engagements for service organizations in a variety of industries. Our SOC services team includes personnel with specialized internal control training and backgrounds. Our professionals have completed the AICPA's SOC School and hold relevant industry certifications. Our professionals help ensure that service organizations receive the highest level of assurance over the effectiveness of their internal controls.

P&N Team Experience & Qualifications: P&N professionals maintain the following certifications related to information technology, data security, internal controls, and compliance:

CISA (Certified Information Systems Auditor)	CIA (Certified Internal Auditor)
CISSP (Certified Info Systems Security Professional)	CITP (Certified Information Technology Professional)
CIPP/US (Certified Information Privacy Professional/United States)	CRISC (Certified in Risk & Information Systems Control)
CIPM (Certified Information Privacy Manager)	Certified HITRUST Practitioner
JNCIS (Juniper Networks Cert. Internet Specialist)	VCP5 (VMware Certified Professional v5)
RSA/CSE (Certified Security Engineer)	VCP6 (VMware Certified Professional v6)
Checkpoint Certified Security Admin	MCITP (Microsoft Certified IT Professional)
MCITP & MCSE - Messaging	MCSE (Microsoft Certified System Engineer)
CCSP (Cisco Certified Security Professional)	CCVP (Cisco Certified Voice Professional)
CCNA (Cisco Certified Network Associate)	CCNP (Cisco Certified Network Professional)
JNCIA (Juniper Networks Certified Associate)	CCDA (Cisco Certified Design Associate)
MCNE (Master Certified Novell Engineer)	BCFP (Brocade Fiber Channel Professional)
BCSD (Brocade Certified SAN Designer)	EnCE (Encase Certified Forensic Examiner)
DOSD (Dell On Site Diagnostics)	AccessData Certified Forensic Examiner

Our security processes follow industry accepted standards such as NIST, HITRUST, CIS Controls; any required elements from regulatory bodies/legislation such as AICPA, HIPAA, HITECH, FFIEC, CUNA, various state requirements; and vendor best practices (i.e. Microsoft, Cisco, VMWare, etc.) We apply the same requirements delivered through our client engagements to our internal processes. Our work product for client engagements have been reviewed, tested, and ultimately accepted by regulatory bodies and government entities such as OCR, FFIEC, and CUNA.

P&N served as an expert in an Office for Civil Rights (OCR) investigation for a HIPAA breach at a large, national covered entity. OCR recognized P&N as "HIPAA Experts" in their final report.

P&N Client Data Hosting & Security: P&N protects its own client data by utilizing data hosting and security services of Venyu, who maintains certified data centers that adhere to the most rigid standards and meet compliance regulations like PCI, HIPAA, FINRA, Sarbanes-Oxley, and Gramm-Leach-Bliley. More specifically, Venyu's facilities include the following security and compliance measures:

- Venyu undergoes a comprehensive annual SSAE16 SOCII audit that tests and verifies all data center, security, business process, and customer management controls.
- Physical security - onsite security personnel, monitoring, video surveillance, biometric and access card, and man-trap access to data center floor.
- Venyu Data Centers have earned the Coalfire badge signifying PCI compliance.
- Venyu Cloud Backup Services and Hosting Services fulfill the requirements of the Health Information Portability & Accountability Act (HIPAA), including data integrity, authentication, contingency planning, and access/audit controls as the relate to electronic Protected Health Information.
- Venyu backup services fulfill the requirements of the Sarbanes-Oxley Act as it relates to record retention, records production, internal controls, and record alteration and destruction.
- FINRA (NASD 3510) require members' business continuity and contingency plans to include procedures to satisfy obligations to clients in the event of an emergency or outage. A key component to any business continuity plan, Venyu delivers remote backup and redundant hosting services to fulfill the requirements of FINRA related to business continuity planning and readiness.

More information can be found at https://www.venyu.com/compliance/.

Venyu Solutions L.L.C. undergoes an annual System and Organizational Controls 2 (SOC 2), Type II exam covering the Security, Confidentiality, Availability, and Processing Integrity Trust Services Categories. P&N has reviewed the most recent independent auditor report and attest that the scope addressed the current SOC 2, Type II trust services criteria for the in scope categories and the audit opinion was unmodified ("clean" opinion), in all material respects. Based on P&N's ongoing vendor monitoring procedures, Venyu's SOC 2, Type II exams have consistently included an unmodified opinion.

General Security Measures: P&N protects data at rest with either encryption or firewalls. Systems that store or transmit personal information have proper security protection, such as antivirus software, with unneeded services or ports turned off and access to needed applications being properly configured. In addition, all employees and personnel that have access to organizational computer systems must adhere to the password policies defined by the firm in order to protect the security of the network, protect data integrity, and protect computer systems. P&N's policy is designed to protect the organizational resources on the network by requiring strong passwords along with protection of these passwords, and establishing a minimum time between changes to passwords.

Two-Factor Authentication: Our proprietary claims management database application utilizes two-factor authentication provided by Duo Security (https://duo.com) for all system users. As described by Duo, *"two-factor authentication adds a second layer of security to your online accounts. Verifying your identity using a second factor (like your mobile phone or other mobile device) prevents anyone but you from logging in, even if they know your password."*

IDS - Ongoing Periodic Security/ Vulnerability Scans and Access and Event Monitoring: P&N's technology services team monitors and manages IDS and IPS alerts in real-time using Checkpoint's Next Generation Firewall to analyze all events and identify threats. Events are correlated across all available information sources, including other IDS and IPS devices, firewall logs, network devices, host and application logs and vulnerability scan results. Risks are responded to immediately so that the threat is countered.

Encryption

Encryption Policy for Confidential Information: P&N utilizes email encryption software. This software allows us to provide a secure method for the transmission of confidential information. Employees are instructed that all emails with confidential data sent outside of P&N's networks must be encrypted. To access email attachments, including financial statements and other confidential documents, a one-time setup of a login and password is required. This allows our clients to be confident that the information we send via email remains confidential and secure.

In addition, any confidential data transmitted through a public network (e.g., Internet) to and from vendors, customers, or entities doing business with P&N must be encrypted or be transmitted through an encrypted tunnel. Confidential data must be transmitted through a tunnel encrypted with VPN or Secure Socket Layer (SSL) technology.

Encrypting Laptop Hard Drives: To protect the confidentiality of client information, the hard drives of all P&N laptops are encrypted with the latest information security technology. This encryption software allows the user a simplified login that opens the encryption and subsequently the Windows software. For the user, the onetime login process is seamless. If the laptop is stolen, the data is not accessible without the login and unscrupulous users are shut out of the system.

Encryption Strength: All encryption mechanisms implemented to comply with this policy must support a minimum of, but not limited to the industry standard of 128-bit encryption.

Mass Data Transmission Through Secure Web Portal: In our efforts to use technology to make our client relationships more effective and efficient, P&N can establish a secure web portal for data transfer on an as-needed basis. Simply put, a secure web portal is a password protected area on our servers that allows users to securely transfer and retrieve information. When transferring a large volume of documents, using a secure web portal is a more efficient practice than traditional methods.

Limited Access to Information: P&N makes every reasonable effort to limit access to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request of information resources.

Data Backup and Recovery: P&N backs up domain controllers, central servers, the entire email system, and certain personal files. Servers are backed up to ensure that files which could become corrupted or deleted may be retrieved. The standard server backup retention/restore time is thirty days. A full backup is performed once a week and will save every file on the server, including the operating system. An incremental backup is performed nightly, except for those nights when a full backup is scheduled, and will save every file that has not yet been saved on a full backup. E-mail servers are backed up in full daily and retained for seven days for disaster recovery use only.

Off-site Storage Policy: In addition, our backups are replicated off-site on a daily basis to P&N's data center hosted by EATEL Business (www.eatelbusiness.com). Our data center is a highly secure facility with alarms, controlled access, fire suppressors, redundant and emergency power generators – everything necessary to ensure valuable customer data is always secure. Additional information related to network and physical security of this data center can be found on EATEL Business's webpage.

Employee Security Protocols Training and Testing: All firm employees are required to complete annual security awareness training. This is a web-based interactive training using common traps, live demonstration videos, short tests and the new scenario-based Danger Zone exercises. The training specializes in making sure employees understand the importance of protecting information like PII and mechanisms of spam, phishing, spear phishing, malware, ransomware and social engineering, and are able to apply this knowledge in their day-to-day jobs. Every new employee is required to complete HIPAA Training and every current employee is required to complete HIPAA Training every other year. All P&N compliance training is maintained in the firm's Learning Management System (LMS) for record keeping purposes.

Quality Control

Our claims administration teams include professionals trained and certified in, among others, the following areas: project management (PMP), accounting (CPA), internal controls and risk (CIA), information systems controls (CISA), fraud examination (CFE), information systems security (CISSP), and legal analysis (JD).

Our project initiation phase includes an identification of critical focus areas and implementation of a plan that covers the following key components of quality control in the context of claims administration service delivery.

Resource Consistency & Training: Because we maintain a large, diverse professional workforce, our team is scalable without the need for temporary employees for every major project. This organic scalability is important in terms of retained process knowledge as well as consistency of execution and deliverables.

Data Validation: P&N implements proactive data validation measures into our online claims platform to minimize claim deficiencies, duplication, and anomalies that require dedication of resources and expenses throughout the claims process.

Segregation of Duties: Segregation of duties is important for risk mitigation and internal control – particularly in the accounting function for large fund projects. The diversity and scalability of our workforce would allow each high risk component of the claims life cycle to be performed by a team member that specializes in the relevant professional area (*rather than a single project manager or assigned resource*).

Technology & Software Analysis Tools: P&N utilizes various software tools to assist in the execution of quality control procedures and identification of suspicious activity. Our systems include "fuzzy" matching logic which allows us to detect and address duplicate claim submissions. We also maintain service subscriptions for technology programs that allow us to research potential fraudulent claim submissions and enables us to report our findings to the parties and Court as appropriate.

Internal Controls: For high risk projects and data sets, our team is able to utilize our Certified Internal Audit (CIA) and other control and risk advisory professionals to design data management and processing protocols that ensure proper internal controls are established.

Fraud, Waste, and Abuse Detection and Prevention

We believe that effective claims administration protocols include fraud detection and prevention but also include mechanisms that combat waste and abuse from legitimate, non-fraudulent sources. P&N uses a variety of techniques to prevent and deter fraud as well as monitor areas that are at high risk for wasteful and abusive claims activity. The following sections outline various methods that we employ to fight fraud, waste, and abuse (FWA) in our claims programs.

Data Validation: One mechanism that helps prevent abuse of the claims process, particularly in a claims process that requires minimal documentation (or no claim support), is to implement a maximum number of "units" that can be claimed without supporting documentation. Enforcing a process in which "high volume" claims follow a particular protocol allows us to easily identify high risk claims and implement particular audit or verification procedures focused on that subset of claim submissions.

It may also be reasonable to establish claim filing rules that help proactively prevent duplicative claim submissions. For example, it may be reasonable to limit claims to one-per-user or one-per-household basis. In this situation, the online claims filing platform may be programmed to reject the submission of claims if a previous claim exists that includes the same attributes such as email address, mailing address, or other information such as serial/model number, etc.

Duplicate Claim Identification: Of course, data validation methods are effective only to the extent that the claim submission rules do not become a barrier to participation. Therefore, it is also necessary to utilize techniques to ensure that duplicate claims are identified after they are submitted.

To meet this need, P&N utilizes technology that includes "fuzzy" matching logic which allows us to detect and address duplicate claim submissions by going beyond exact matches and analyzing claims that have similar characteristics across a number of fields. For example, we may compare claims that have a combination of 90% commonality amongst the claimant name and 95% match for mailing address (and vice versa). *Using these techniques across different claimant attributes has allowed us to identify thousands of duplicative claims that otherwise do not appear suspicious.*

Data Analytics: Another method that helps to identify potential FWA activity is the use of data analysis. Our business intelligence professionals utilize custom reporting to identify anomalies in large claims datasets and assess those outliers. We utilize exception reporting to capture scenarios that exist within the data (but should not reasonably be possible) so that we can take appropriate corrective action as needed.

Research Tools: P&N maintains service subscriptions for technology programs that allow us to research potential fraudulent claim submissions and enables us to either confirm the legitimacy of claim information or document findings so that we can report to the parties and Court as appropriate.

The following examples illustrate our experiencing in employing fraud detection and prevention tools and processes in the class action settlement environment:

CRT Antitrust Litigation

P&N helped establish various thresholds for claims audit procedures as well as executed many different claims analysis processes to identify high risk or suspicious claims activity.

To date, P&N's efforts have resulted in a recovery of over $100 Million in settlement fund value. We have achieved significant results related to (a) ineligible claim withdrawals, (b) duplicate claim identification, (c) adjustments resulting from completed claim audits, and (d) FWA procedures. The value of the recovery is determined by the total per-unit dollar value ***increase*** of all units which remain in the settlement program as a result of the claims review process.

Deepwater Horizon Economic Claims Center (DHECC)

P&N provided personnel to help create the fraud, waste and abuse (FWA) team for this program. This team managed and oversaw the investigative review process of potentially fraudulent Business Economic Loss and Seafood claims.

Engineering the Process – P&N created the investigative work plans, consistency guidelines and a quality checklist to drive uniformity of each investigation. The guidelines documented standard language, management decisions, investigation requirements, scope and best practices.

Predictive Analysis (Statistical Analysis Software, or SAS) – Our analysts recommended data points and metrics for predictive modeling and anomaly detection within the data analytics software used to automate the way in which potentially fraudulent claims were identified. Our team tested the weighted business rules used to score claims based on where they fell on a spectrum, which allowed for the prioritization of claims with a higher likelihood of fraud.

Investigation & Reporting – P&N's FWA team performed a thorough investigation of the financial records for claims identified by SAS in addition to internal and external referrals as having indicia of fraud. Investigations included review of documentation germane to claim, identification and investigation of red flags, and outreach to claimants or third parties, as necessary. The fraud team created a summary of fraud findings for each claim utilizing analysis and state and federal databases. Analysts prepared detailed court documents for appeals panelists in the event claimants appealed the initial findings, and circulated internal reports of possible organized fraud schemes.